UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. MURUGANANANDAM ARUMUGAM, Defendant.	Case No. 19-CR-41-RSL ORDER DENYING DEFENDANT'S MOTIONS TO SUPPRESS

This matter comes before the Court on defendant's "Motion to Suppress Evidence" (Dkt. #43) and "Motion to Suppress Physical Evidence" (Dkt. #44). The Court heard argument and testimony from the parties on March 3, 2020.

I. FACTUAL BACKGROUND

Defendant Murugananandam Arumugam is charged with one count of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B), (b)(2), and one count of receipt of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), (b)(1). See Dkt. #84 (Second Superseding Indictment). He moves to suppress evidence and all fruits of evidence seized as a result of the government's use of RoundUp eMule software, and as a result of a February 1, 2018 search warrant executed on his residence.

a. RoundUp eMule

This case involves the government's use of a software program called RoundUp eMule (hereinafter "RoundUp") to investigate defendant's activity on a peer-to-peer ("P2P") file sharing network. The government uses RoundUp to conduct surveillance on a public P2P

network called eMule, which is used by millions of individuals for both lawful and unlawful purposes. See Dkt. #43 (Ex. B) (Lahman Decl.) at 3; Dkt. #61-2 (Lynn Decl.) at ¶ 3.[1] RoundUp is a modified version of eMule (hereinafter "standard eMule"), a public, open-source P2P network.

The eMule P2P network allows users to share files, including videos, audio, pictures, text, and any other type of file. See Lynn Decl. at ¶ 3; Lahman Decl. at 5. Unlike earlier sharing networks, which required files to be held on a centralized server for download, P2P networks allow users to acquire files directly from other network users. Lynn Decl. at ¶ 3; Lahman Decl. at 2. The network breaks up a file that is being shared by downloading different "parts" of the file from different users on the network at the same time. Lynn Decl. at ¶ 6.

To use a P2P network, an individual must download and install a "client" program onto their computer. Id. at ¶ 5. The client provides a user interface that allows users to search for, share, and download files on the P2P network. Id. The eMule client is the program used to navigate the P2P network. Id. at ¶ 4. When an individual user installs an eMule client, one or more file folders become designated as "shared" folders. Id. at ¶ 6. The files in a user's shared folder will be made available to the other users on the eMule network for sharing. Id. The functionality of eMule depends on the exchange of computer IP addresses, because the addresses allow users to communicate and share files with each other. Id. at ¶ 10; cf. Lahman Decl. at 5.

RoundUp is a modified version of standard eMule, which law enforcement uses to conduct undercover child pornography investigations. Lynn Decl. at ¶ 21; Lahman Decl. at 3. Although RoundUp "retains much of the functionality" of standard eMule, it is enhanced in what its developer Brian Lynn recognizes as four key areas. Lynn Decl. at ¶ 22. First, RoundUp does not share any of the files it downloads, which prevents further dissemination of contraband files across the P2P network. Id. at ¶ 32. Second, RoundUp is coded to download

[1] This Order collectively references the eMule P2P network, which the Court understands to incorporate the original eDonkey2000 network and client capabilities. See Lahman Decl. at 3; Lynn Decl. at ¶ 4.

from a single source download candidate, so that a download can be attributed to a single user on the eMule network. Id. at ¶ 33. This contrasts with standard eMule, which is specifically designed to download portions of files from multiple download candidates. Id. Third, RoundUp generates download logs, which catalog whether (1) RoundUp connects to the intended IP address, (2) the downloaded file is the intended file and has been downloaded without file corruption, and (3) the recorded download time is accurate. Id. at ¶ 35. This allows RoundUp users to validate these elements of a single source download. Id. Finally, RoundUp can search the eMule network for files identified by law enforcement as associated with child pornography. Id. at ¶ 36. RoundUp accomplishes this by reading a list of "eD2k file hashes"[2] of previously identified files, and then searching the network for IP addresses of users who have announced interest in or have possession of files with those hashes. Id.

b. Investigation and Procedural History

The material facts underlying the government's investigation of defendant are largely undisputed. From approximately July 9, 2016 to April 17, 2017, Seattle Police Department Detective Daniel Conine used RoundUp to investigate an eMule user at IP address 73.11.164.229, Port 54494. See Dkt. #43 (Ex. D) at 11. Between August 24, 2016 and April 12, 2017, Detective Conine used RoundUp to successfully download 2,942 files or partial files from the IP address. Id. (Ex. G) at 17.

Detective Conine conducted a public search and learned that the IP address belonged to Comcast. Id. (Ex. D) at 14. He sought a warrant in King County Superior Court to determine who subscribed to the IP address. Id. In his affidavit in support of the Comcast warrant, Detective Conine described two videos that were among the 2,942 files he downloaded. Id. at 11-14. First, Detective Conine described a single source connection to the IP address on August 24, 2016, as well as his observation that defendant was in possession of and sharing 40 of 68 parts of a known child pornography video depicting the repeated rape of a prepubescent female

[2] RoundUp developer Brian Lynn describes file hashes as "ubiquitous in computer science" and likens a file hash to a digital fingerprint. See Lynn Decl. at ¶ 12. Any two files with the same hash value can be expected to be identical files. Id. at ¶ 13.

child. Id. Second, Detective Conine described a single source connection to the IP address on April 12, 2017, as well as his observation that defendant was in possession of and sharing 9 of 11 parts of a known child pornography video depicting a prepubescent female child being raped by an adult man and an adult woman. Id. King County Superior Court Judge Helen J. Halpert signed the Comcast search warrant on April 20, 2017. Id. at 16. Detective Conine obtained the subscriber information from Comcast and determined that defendant was the subscriber of the IP address.

On January 30, 2018, Sergeant Bradley C. Turi of King County Sheriff's Office sought a search warrant for a residence in Redmond, Washington. Dkt. #45 (Ex. G). In support of the warrant, Sergeant Turi incorporated by reference Detective Conine's Comcast affidavit. Id. King County Superior Court Judge Catherine Moore issued the residential search warrant on January 30, 2018. Id. at 23.

On February 1, 2018, Sergeant Turi and a team of Internet Crimes Against Children Taskforce officers executed the search warrant at defendant's residence. Dkt. #43 (Ex. I). They recovered a computer and storage devices from the residence. Id. A forensic examination of the computer confirmed the presence of eMule software and files depicting child pornography.

II. FIRST MOTION TO SUPPRESS (Dkt. #43)

In his first motion to suppress, defendant seeks to suppress all evidence and all fruits of that evidence that the government seized as a result of its use of RoundUp. Dkt. #43. He alleges that a warrantless search occurred when the government "engaged in a generalized surveillance" using technology not available to the general public. Id. at 1. He also contends that the government's use of RoundUp constituted an unlawful "digital trespass" onto his computer. Id.

a. Legal Standard

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. The threshold question is whether a Fourth Amendment "search" has occurred. See Kyllo v. United States, 533 U.S. 27, 31 (2001). "[G]overnment

conduct qualifies as a search only if it violates a reasonable expectation of privacy." United States v. Borowy, 595 F.3d 1045, 1047 (9th Cir. 2010) (citing Katz v. United States, 389 U.S. 347 (1967)).

b. Generalized Surveillance Using Technology Unavailable to the Public

Defendant alleges the government's use of RoundUp constituted a search because the technology incorporates several modifications to standard eMule, and is accordingly "not in general public use." Dkt. #43 at 11-14. He also argues that eMule users do not expect or consent to having their eMule activities recorded and aggregated by the government. Id. The government counters that the Fourth Amendment does not shield public file sharing on the internet. See Dkt. #60 at 5-10. It asserts that defendant had no reasonable expectation of privacy in his computer because he joined eMule, a public file sharing network, and installed software that allowed him to affirmatively obtain and share files. Further, the government argues that the modifications to eMule inherent in RoundUp do not make it "a device that is not in the general public use." Id. at 7-10.

In recent decades, the Supreme Court has rejected a "mechanical interpretation" of the Fourth Amendment. See Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citation omitted). As technology has in evolved in ways impacting the privacy rights and expectations of Americans, so has Fourth Amendment jurisprudence. See, e.g., Kyllo, 533 U.S. at 27 (finding search in government's use of thermal imaging technology not in public use to explore private details of home); United States v. Jones, 565 U.S. 400 (2012) (finding search in placement of a GPS device on a target's vehicle); Riley v. California, 573 U.S. 373 (2014) (finding search in officer's access of smart phone data including text messages, contacts, and photo and video files); Carpenter, 138 S. Ct. at 2216-17 (2018) (finding search in government's use of cell-site location information ("CSLI") records and noting the "unique nature" of cell phone information, including the ability to track an individual's physical location). While the Court is cognizant of the evolving and delicate nature of the Fourth Amendment as intertwined with technological advancement, defendant now asks the Court to expand the Constitution's privacy guarantees farther than any court has before: to the P2P file-sharing network context.

The Court, having considered the parties' arguments and the existing weight of authority, is not persuaded to do so.

Although Carpenter emphasized that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere," it qualified this extension of the reasonable expectation of privacy to "what [one] seeks to preserve as private, even in an area accessible to the public." Id. at 2217. Although an eMule user may affirmatively download and utilize software on his personal computer, the program's key functionality involves public access to, sharing, and downloading of online files. The Court agrees that "[a]ccessing files in a 'shared' folder does not violate the Fourth Amendment because no reasonable expectation of privacy exists with regard to such files." See United States v. Blouin, 2017 WL 3485736, at *2 (Aug. 15, 2017) (citations omitted); see also United States v. Dreyer, 804 F.3d 1266, 1278 n.6 (9th Cir. 2015) (internal quotation marks and citations omitted) ("[A]ccessing files made available through [a P2P] file-sharing software does not constitute a search, . . . [because] when an individual uses a file-sharing software, he opens his computer to anyone else with the same freely available program, thereby opening up his download folder to the world."); United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (recognizing that "as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer," but "fail[ing] to see how this expectation c[ould] survive [the defendant's] decision to install and use [P2P] file-sharing software, thereby opening his computer to anyone else with the same freely available program").

RoundUp, software with certain technological modifications to a public, open-source P2P network sharing client, is designed to access public files that individuals affirmatively place into the public sphere. Defendant had no reasonable expectation of privacy in the files he chose to upload to his eMule "shared" folder for public download. Accordingly, the government's use of RoundUp to access his public files did not constitute a Fourth Amendment "search."

c. "Digital Trespassing"

Defendant also argues that the government placed a "tracer tag on the target computer and downloaded a partial file from the target computer." Dkt. #43 at 14-16. In doing so,

defendant claims, the government "digitally trespassed" into the device connected to his IP address. Id. Defendant alleges that the government placed this "tracer tag" on his computer approximately 3,000 times in eight months. Id. Defendant equates this to monitoring of his IP address, which he asserts he never agreed to. Id.

The Court is not persuaded by defendant's speculative "tracer tag" allegations. RoundUp developer Brian Lynn explains that what defendant describes as a "tracer tag" is simply information recorded by his own eMule client when he shares his publicly stored files with the RoundUp eMule client. Lynn Decl. at ¶¶ 26-28, 41-52. Lynn also explains that the eMule client would have stored certain information, such as the particular user hash identifier of Detective Conine's RoundUp client, or any other eMule client that he shared files with.[3] Lynn Decl. at ¶¶ 41-52. While the act of storing this information has been referred to as "tagging," see Dkt. #62, Lynn explains that defendant's eMule client behaved just as it would have if anyone else had connected to it to download files from the eMule network. Id. RoundUp did not "do" anything to defendant's computer—rather, the eMule program defendant chose to download registered the connections to other clients, including Detective Conine's RoundUp client. Id.; cf. Jones, 565 U.S. at 404 (emphasizing the government's physical occupation of private property for purposes of obtaining information). Defendant has not established any purported "digital trespass" in the government's use of RoundUp, and has not shown that any Fourth Amendment search occurred. Defendant's first motion to suppress (Dkt. #43) is DENIED.

d. Request for Franks Hearing

Defendant also requests a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978). He alleges that Detective Conine misrepresented and omitted facts from the affidavit accompanying his warrant application that were material to a finding of probable cause. He

[3] Lynn also elaborates on eMule's optional "Secure User Identification" setting, which is available to every eMule user and is used to verify that one user is not impersonating another. Lynn Decl. at ¶ 43. Even if the setting were disabled, an interacting eMule client would record a user hash identifier. Id. at ¶ 44. Because the Secure User Identification setting was enabled on defendant's computer, his eMule client recorded additional information, namely the public key associated with Detective Conine's user hash. Id. at ¶¶ 48-49.

argues that Detective Conine failed to indicate that he used an automated system to connect with and download files from IP Address 73.11.164.229, Port 54494, or to detail any potential reliability concerns with the program. Id.

An affidavit supporting a search warrant is presumptively valid. See Franks, 438 U.S. at 171. Further, "[p]robable cause does not require certainty and demands even less than probability." Blouin, 2017 WL 3485736, at *3 (internal quotation marks and citations omitted). However, "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." Franks, 438 U.S. at 155-56.

At least three district courts (including this one) have rejected the Franks arguments regarding the automated nature and reliability of RoundUp that defendant now raises. The Blouin court discounted the alleged omission of details regarding the automated nature of RoundUp, and concluded "as a matter of law that, if files with hash values known to be associated with child pornography are reported to be on the 'shared' folder of a suspect's computer, probable cause exists for searching such suspect's computer." Blouin, 2017 WL 3485736, at *4. Further, in United States v. Feldman, 2014 WL 7653617, at *7 (E.D. Wis. July 7, 2014), the Eastern District of Wisconsin concluded that "the fact that the investigation may have occurred automatically rather than through the manual manipulation of an investigator is [not] relevant to the court's assessment of probable cause." Id. Finally, in United States v. Case, 2014 WL 1052946, at *4 (E.D. Wis. Mar. 17, 2014), the court noted that "[e]ven assuming that the program was running unattended at the time of the downloads, defendant provides no authority in support of his claim that this precludes a finding of probable cause." The Court agrees with the reasoning of these analogous cases, and concludes that any omissions in the affidavit regarding technical details of RoundUp and its automated operations were not material to the probable cause inquiry. Further, the Court concludes that any alleged concerns as to RoundUp's reliability are speculative. RoundUp was used to download video files, which

Detective Conine confirmed depicted child pornography and described in detail in his affidavit. See Case, 2014 WL 1052946, at *3-4 (finding similar process "sufficiently reliable to support the issuance of the warrant").

Defendant has not made the "substantial preliminary showing" required for a Franks hearing. See Franks, 438 U.S. at 155-56. Accordingly, his Franks request is DENIED.

III. SECOND MOTION TO SUPPRESS (Dkt. #44)

In his second motion to suppress, defendant seeks suppression of physical evidence seized during the February 2, 2018 search warrant executed on his residence. See Dkt. #44. This evidence includes "all computers, computer devices, and images recovered from the search of those computer devices," as well as all statements made following the execution of the search warrant. Id. at 1. Defendant argues that the search warrant was not supported by probable cause and accordingly violated the Fourth Amendment.

a. Legal Standard

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV. Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." Ornelas v. United States, 517 U.S. 690, 696 (1996) (citations omitted). A finding of probable cause requires only a "fair probability that contraband or evidence is located in a particular place," which in turn depends on "the totality of the circumstances, including reasonable inferences, and is a common sense, practical question." United States v. Kelley, 482 F.3d 1047, 1050 (9th Cir. 2007) (internal quotation marks and citation omitted). "[T]he preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination." United States v. Leon, 468 U.S. 897, 914 (1984). However, a reviewing court "should find that probable cause is not met when the issuing judge lacked a 'substantial basis' for concluding that probable cause existed." United States v. Underwood, 725 F.3d 1076, 1081 (9th Cir. 2013) (internal quotation marks and citations omitted).

b. Probable Cause

Defendant argues that the residential search warrant was not supported by probable cause because it relied on (1) descriptions of only two child pornography files associated with defendant's IP address, and (2) descriptions of common traits of child pornography "collectors." See Dkt. #44 at 4-8. He likens the two videos detailed in the affidavit to "sporadic evidence" of access to child pornography, focusing on the fact that 2,942 files were downloaded, while only two were described. He also highlights the fact that the last download from his IP address occurred on April 12, 2017, almost ten months before the search warrant was executed on his residence. Defendant argues that, without the affidavit's description of common propensities of child pornography "collectors," including that they often maintain the pornographic material for many years, the ten-month old file download evidence would have been too stale to support probable cause.

To support his arguments, defendant relies heavily upon a Second Circuit case, United States v. Raymonda, 780 F.3d 105 (2d Cir. 2015). But Raymonda, which is not binding on this Court, is factually inapposite. In Raymonda, the Second Circuit held that a warrant was not supported by probable cause because a single instance of online access to child pornography did not create a fair probability that child pornography would be found on the defendant's computer eight months after all traces of that online access had likely cleared. Id. at 116-17. The sole evidence underlying the warrant in Raymonda was a single occasion in which defendant's IP address accessed a webpage containing 76 thumbnail images of child pornography over a period of 17 seconds. Id. at 110. The IP log showed no user requests for any full-sized versions of the thumbnails during the brief time period. Id. The affidavit supporting the warrant application described this single incident of access and included descriptions of common characteristics of child pornography "collectors." Id. at 110-11.

Here, the affidavit described law enforcement's downloading of 2,942 files or partial files. See Dkt. #44-1 (Ex. A) at 18. And while the affidavit did not explicitly state that these files constituted child pornography, it provided detailed descriptions of two graphic, lengthy video files depicting adults raping minor children. Id. at 19-20. Further, it described

defendant's decision to affirmatively download the eMule client and make the video files available for public download. This affirmatively shared video evidence amounted to more than a single, 17-second, potentially inadvertent online access of thumbnail images. See Raymonda, 780 F.3d at 115 ("Courts have [] inferred that a suspect was a hoarder of child pornography on the basis of a single incident of possession or receipt . . . where, for example, the suspect's access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files.").

Moreover, the Ninth Circuit has affirmed probable cause determinations on similar facts. For example, in United States v. Lacy, 119 F.3d 742 (9th Cir. 1997), a defendant affirmatively downloaded two GIF files depicting child pornography ten months before a warrant issued. Id. at 745. The Ninth Circuit upheld the district court's determination that the downloads, coupled with the affiant's description of characteristics of child pornography collectors, were sufficient to support a probable cause finding. Id. at 745-46. United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013) is also persuasive. While the defendant in Schesso had "essentially conceded probable cause" before the district court as to most of the devices seized from his residence, the Ninth Circuit nevertheless concluded that there was "no question that there was probable cause to believe [he] possessed the particular child pornography video" based on his upload to the eDonkey network of a child pornography video 20 months before, and the affiant's description of characteristics of child pornography collectors. Id. at 1043, 1045-46 ("These factors . . . justify the seizure and subsequent off-premises search of Schesso's entire computer system and associated digital storage devices.").

Here, considering the totality of the circumstances, there was "a fair probability that contraband or evidence of child pornography would be found on [defendant's] computer[.]" See Schesso, 730 F.3d at 1046 (internal quotation marks omitted) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). Further, combined with the information in the affidavit, the approximately ten-month gap between the file downloads and warrant's issuance did not render the evidence stale. See Schesso, 730 F.3d at 1047 (citing Lacy, 119 F.3d at 745-46) (citation

omitted). The Court concludes that the residential search warrant was supported by probable cause. Defendant's second motion to suppress (Dkt. #44) is DENIED.[4]

IV. CONCLUSION

For all the foregoing reasons, defendant's motions to suppress (Dkts. #43, 44) are DENIED. Defendant's request for a Franks hearing is also DENIED (Dkt. #43).

DATED this 10th day of March, 2020.

Robert S. Lasnik
United States District Judge

[4] Because the residential search warrant was supported by probable cause, the Court need not reach the parties' arguments as to the applicability of the "good faith" exception, which counsels that suppression is improper where an officer acts "in objectively reasonable reliance on the warrant." Leon, 468 U.S. at 922. Regardless, defendant has not persuasively established the existence of any of the four identified circumstances that *per se* fail to satisfy the good faith exception. See Underwood, 725 F.3d at 1085.